Japanese Patent No. 2606827

Issue date : February 13, 1997

Applicant : Kabushiki Kaisha Toshiba

Title : February 13, 1997

Specifically, each terminal is provided with an encryption/decryption function and, at the sending end, the sender uses his/her own keyword to encrypt a message to be communicated according to the encryption program. The encrypted message is then transmitted to a terminal at the receiving end over the communication line. At the receiving end, a keyword specific to this particular sender stored in the key memory is used, the encrypted message received is decrypted by the decryption circuit and recorded.

If it is assumed that the keyword stored in the key memory is managed to prevent it from leaking outside and that the receiver does not commit fraud such as communication document forgery, this means that there is no one but the sender knowing the keyword who can create the encrypted message recorded. Therefore, in this case, the encrypted message recorded at the receiving end is highly admissible as evidence making a digital signature for communication documents reality.

Fig. 1 schematically depicts the IC card functionality. The actual hardware architecture is as described above and

implements different functions as follows.

As mentioned above, the present embodiment uses an IC card as an encryption device. The IC card comprises encryption circuits 2a, 2b and decryption circuits 5a, 5b. By definition, the encryption circuits 2a, 2b represent a function that converts a plaintext into a message on a communication line while decryption circuits 5a, 5b represent a function that converts a message on the communication line into a plaintext.

Data is input to the encryption circuit 2a from a higher-level processing device or the reader/writer 27 via a combining unit 4a. The combining unit 4a combines a plaintext from the reader/writer 27 with an identification word and provides the result to the encryption circuit 2a. The combination here is a serial combination that combines a bit string that is for example a plain text with an identification word. The serial combination herein means that a bit string representing an identification word is added at the position immediately after a bit string representing a plaintext to produce a new bit string, and more specifically means that, as shown in Fig. 7, an identification number N (n bit(s)) is added at the position immediately after a transaction message M (m bit(s)) to form a new bit string of (m+n) bits.

The identification word is stored in an identification word register 3a, and the register 3a is sealed inside the IC card with other components.

Along with this identification word register 3a, a key register 1a is provided and a "key" is stored in the register 3a. The "key" defines encryption and decryption algorithms in the encryption circuit 2a and the decryption circuit 5a. Technologies such as the DES system can be used for the encryption and decryption.

Data encrypted with the "key" is provided to the outgoing communication from the IC card. It is then received by another IC card provided as a counterpart.

It is then decrypted in the decryption circuit 5b. The resulting data is provided to the higher-level processing device or the reader/writer, detached therefrom of the identification word, and undergoes a specified process.

In the description above, certification of contents associated with a message from the user to the center is discussed. In exactly the same manner, it is also possible to certify a message delivery from the center by recording the encrypted message from the center at a terminal on the user side. This is achieved by an identification number N', which is specific to the IC card at the center side that is added to a message, when the message is encrypted inside the IC card at the center side.

(19)日本国特許庁（ＪＰ）　(12)特　許　公　報（Ｂ２）　(11)特許番号

第2606827号

(45)発行日　平成９年(1997)５月７日　(24)登録日　平成９年(1997)２月13日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０９Ｃ　1/00	６１０	7259－５Ｊ	Ｇ０９Ｃ　1/00	６１０Ｚ
	６６０	7259－５Ｊ		６６０Ａ
Ｈ０４Ｋ　1/02			Ｈ０４Ｋ　1/02	

発明の数１（全 11 頁）

(21)出願番号　特願昭61－172736

(22)出願日　昭和61年(1986)７月24日

(65)公開番号　特開昭63－29785

(43)公開日　昭和63年(1988)２月８日

審判番号　平7－2634

(73)特許権者　999999999
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　神竹　孝至
川崎市幸区小向東芝町１　株式会社東芝
総合研究所内

(72)発明者　川村　信一
川崎市幸区小向東芝町１　株式会社東芝
総合研究所内

(74)代理人　弁理士　外川　英明　（外１名）

合議体
審判長　菅野　嘉昭
審判官　稲葉　慶和
審判官　斎藤　操

最終頁に続く

(54)【発明の名称】　ＩＣカードを用いた暗号装置

1

(57)【特許請求の範囲】

【請求項１】入力情報を暗号化するためのカギ情報を格納する第一の手段と、ICカードに固有の識別情報を格納する第二の手段と、前記入力情報と前記識別情報とが再分離可能な状態で合成された情報を第一の格納手段に格納されたカギ情報に従って暗号化する手段とを含むICカードと、

前記ICカードにより暗号化された情報を復号する復号手段と、復号された情報を前記入力情報と前記固有の識別情報とに分離する手段と、ICカードに固有の識別情報を予め保管する手段と、前記復号された情報から分離した識別情報と前記保管手段に保管された識別情報とを比較することにより相手装置を確認する手段とを含む端末装置とからなるICカードを用いた暗号装置。

【請求項２】第一の格納手段、第二の格納手段及び暗号化手段を前記ICカード内に封止する封止手段を更に具備したことを特徴とする特許請求の範囲第１項記載のICカードを用いた暗号装置。

2

【請求項３】前記カギ情報は、ICカードを使用する者毎に設定された符号と、入力情報の通信に先立って前記端末装置から送信された符号とを用いて生成されることを特徴とする特許請求の範囲第１項記載のICカードを用いた暗号装置。

【請求項４】前記ICカードは、入力情報の通信に先立ってその通信毎に固有の取引信号を付与する手段を含み、前記暗号化手段は、前記入力情報と前記ICカードに固有の識別情報と前記通信毎に固有の取引情報とを再分離可能な自体で合成した後、第一の格納手段に格納されたカギ情報に従って暗号化することを特徴とする特許請求の範囲第１項記載のICカードを用いた暗号装置。

【発明の詳細な説明】

［発明の目的］

（産業上の利用分野）

この発明は、オンライン取引システム等において、取引を安全確実に実現するための暗号装置に関する。

（従来の技術）

近年、電子技術の進歩に伴いホームバンキング、ホームショッピング、ファームバンキングシステムのような進歩した通信ネットワークシステムの開発が進められている。このような金銭の取引に関係した通信ネットワークシステムを実現する際の最も留意すべき点は、ネットワーク上における取引の秘密および安全性を十分に確保し得ることである。つまり、ネットワークを介在させた取引者間の取引あるいは文書通信においては、取引書や通信文書の証拠能力を高めることが必要である。

ところで通信ネットワークを利用した取引や文書通信における典型的な不正は以下のようなものである。

（１）虚偽申告；送信者（sender）が真に送信したにも拘らず、送信者が受信者側に送信しなかったと申告すること。また送信者が送信しなかったにも拘らず、受信者側に送信したと申告すること。

（２）取引書類の偽造；受信者側に記録されている通信文書を受信者が勝手に書換え、または通信文書を受信者が勝手に作ること。

これらの不正は金銭の横領等の不正につながる。

そこでネットワーク上でのこのような不正を防止するべく、通信ネットワークの各端末にDES（Data Encryption Standard）方式のような暗号化プログラムを内蔵させることにより通信文書の偽造を極力防止することが考えられている。

即ち、各端末に暗号化（encryption）／復号化（decryption）機能を設け、送信側において送信者は自己のキーワードを用いて通信されるべき電文（message）を暗号化プログラムに従って暗号化する。そしてこの暗号電文を通信回線を介して受信者側端末に送信する。そして受信者側においては、キーメモリーに記憶された送信者に固有なキーワードを用い、復号化回路により受信された暗号電文を復号すると共に、これを記録するようにする。

従って、仮に受信側においてキーメモリに記録されたキーワードが外部に漏洩しないように管理し、且つ受信者が通信文書の偽造のような不正を行なわないと仮定できるならば、記録された暗号電文を作成できるのはキーワードを知っている送信者以外には存在しないことになる。故に、この場合には受信者側に記録された暗号電文の証拠能力は高く、ここに通信文書のデジタル署名が可能となる。

然し乍ら、通信者が受信端末の動作モードを復号化モードから暗号化モードに切換えれば、送信者のキーワードを使用して暗号化電文を不正に作成することは可能である。

このように、暗号化／復号化方式に基づいた通信ネットワークシステムにあっては、送信側および受信側の双方で不正を完全に防止することはできない。この為、取引の安全を確保することが困難である。

（発明が解決しようとする問題点）

本発明はこのような事情を考慮してなされたもので、その目的とするところは、通信情報に対する確実なディジタル署名を可能ならしめて、例えば商取引や文書通信の安全性を十分に確保することのできる通信システムを提供することにある。

［発明の構成］

（問題点を解決する為の手段）

この発明は、入力情報を暗号化するためのカギ情報を格納する第一の手段と、ICカードに固有の識別情報を格納する第二の手段と、前記入力情報と前記識別情報とが再分離可能な状態で合成された情報を第一の格納手段に格納されたカギ情報に従って暗号化する手段とを含むICカードと、前記ICカードにより暗号化された情報を復号する復号手段と、復号された情報を前記入力情報と前記固有の識別情報とに分離する手段と、ICカードに固有の識別情報を予め保管する手段と、前記復号された情報から分離した識別情報と前記保管手段に保管された識別情報とを比較することにより相手装置を確認する手段とを含む端末装置とからなるICカードを用いた暗号装置を提供するものである。

（作用）

通信電文は、暗号化される際には、必ず、暗号装置を識別する情報が付加された後に、暗号化される。よって、受信側では、復号後、識別情報を調べることによって、電文を暗号化した装置（発信元）を特定することが可能となる。また、暗号文を復号せずに記録しておくことによって、電文の内容と、その発信元を示す証拠として用いることができる。

（実施例）

以下、図面を参照して本発明に係る一実施例システムにつき説明する。

この実施例では、暗号装置としてICカードを用いている。

第２図はホームバンキング、ホームショッピング、ファームバンキングシステム等に適用され、暗号化／復号化機能を備えたICカードを用いて暗号化通信を行う通信ネットワークの概略的構成図である。

この通信ネットワークは（n:1）のシステムを構成している。例えば家庭や企業等にそれぞれ設置された複数の顧客側端末11a, 11b, ～11nは通信回線13a, 13b, ～13nをそれぞれ介して銀行やデパートメントストアなどの唯一つのセンタに設置されたセンタ側端末12に接続される。

この実施例では、顧客側端末11a, 11b, ～11nからセンタ側端末12に取引電文Mが送信される。

5

顧客側端末11a, 11b, ～11nにはそれぞれ暗号化装置である携帯可能なICカード14a, 14b, ～14nが挿入可能な形態で付属している。またセンタ側端末12にも復号化装置である携帯可能なICカード15が挿入可能な形態で付属している。

第３図はこのような顧客側端末の構成を示すものである。端末11a, 11b, ～11nは、基本的にパーソナルコンピュータのような情報処理装置で構成される。一方、センタ側端末にも、ほぼ同様な構成をとっているが、センタ側では、各ユーザ情報をデータベース39に備えている（第４図参照）。

中央処理装置（CPU）21, 31には通常のパーソナルコンピュータと同じように、制御プログラムを蓄積したメモリ22, 32, 入力装置を構成するキーボード23, 33, および出力装置を構成するCRT表示装置24, 33, とプリンタ25, 35, およびフロッピーディスク装置26, 36等が接続されている。

ICカード14（15）が装填されるカードリーダ／ライタ27, 37はCPU21, 31に結合され、CPU21, 31からの情報をICカード14（15）に供給し、またICカード14（15）の情報をCPU21, 31に供給するものである。尚、CPU21, 31はモデム28, 38を介して通信回線に結合されている。

ICカード14（15）は内部に半導体大規模集積回路を密封して構成され、特定の情報（暗号通信された情報）以外の情報を外部に取出すことができないように構成されている。

本発明のシステムで使用されるICカードは良く知られて従来のICカードと同じ基本構成を有しており、例えば第５図に示すように、マイクロ・プロセッサ・ユニット（MPU:one－chipmicroprocessor）41と、暗号化（復号化）プログラムおよび動作プログラムを内蔵したプログラムメモリ42（マスクROMが好ましい）と、データメモリ43（永久記憶型のPROMまたはEPROMが好ましい）と、I/Oインターフェース44、およびコンタクト部45を備えて構成される。

カードリーダ／ライタ27, 37は、そこにICカード14（15）が装填されたとき、コンタクト部45を介して外部から動作電源電圧、動作クロックパルス、各種機能コマンドコードおよびデータを供給する。尚、MPU41はその内部にRAM41aを備えている。

プログラムメモリ42は、ICカードの基本機能を実行させる各種プログラムを蓄積している。このICカードの基本機能は、①データメモリ43からデータを読出し、または該データメモリ43にデータを書込む機能、②通信回路を介して他の端末に電文を送信する時に通信電文の漏洩や偽造を防止するために電文を暗号化し、また受信した暗号化電文を復号化する暗号化／復号化機能、および③ユーザおよび端末、ホスト等ICカードの通信相手の正当性の確認を行う機能から成る。

MPU41は前記CPU21, 31からカードリーダ／ライタ27, 37

6

を介して入力された機能コマンドコード、またはデータが付加された機能コマンドコードを解釈して上記基本機能のうち必要な機能を選択して実行する。

カードリーダ／ライタ27, 37はICカード14（15）とCPU21, 31との間で機能コマンドコードやデータの授受をおこない、CPU21, 31からのマクロ命令をICカード用のコマンドに分解し、これらコマンドをICカードに供給するものとなっている。

以上がシステム構成の概要であるが、次に、このシステムにおけるICカード同士の通信について説明する。

第１図ではICカードの機能を模式的に表わしている。実際のハードウェア構成については上記のとおりであって、下記の諸機能を実現している。

前述のようにこの実施例では、暗号装置として、ICカードを採用している。ICカードは、暗号化回路2a, 2b, 復号化回路5a, 5bを有している。定義上、暗号化回路2a, 2bは、平文を回線上の電文に変換する機能を指し、復号化回路5a, 5bは、回線上の電文を平文に変換する機能を指す。

暗号化回路2aには、上位の処理装置又は、リーダ／ライタ27から、合成手段4aを介してデータが入力される。合成手段4aでは、リーダ／ライタ27からの平文に、識別ワードを合成して、暗号化回路2aに供給している。ここでの合成しては、例えば平文であるビット列に識別ワードを直列合成している。ここで直列合成とは、平文であるビット列の直後に識別ワードのビット列を付加して新たなビット列を生成することであり、具体的には第７図に示す通り、取引電文Ｍ（ｍビット）の直後に識別番号Ｎ（ｎビット）を付加して新たに（ｍ＋ｎ）ビットのビット列を構成することをいう。

識別ワードは、識別ワードレジスタ3aに記憶されており、該レジスタ3aは、他の構成要素と共に、ICカード内に密封されている。

この識別ワードレジスタ3aと共に、鍵レジスタ1aが設けられており、このレジスタ3a内には、“鍵”が記憶されている。この“鍵”が暗号化回路2a, 復号化回路5aでの暗号化、復号化のアルゴリズムが規定される。暗号化、復号化に用いる技術は、例えば、DES方式等を用いれば良い。

“鍵”により暗号化されたデータは、ICカード外へ送出された通信に供される。そして、対向して設けられたICカードにより受信される。

そして復号化回5bにおいて、復号される。このデータは、上位の処理装置、リーダ／ライタへ供給され、識別ワードが分離され所定の処理が施される。

このようにすることによって以下、効果が得られる。

① 識別ワードをICカード固有のものに設定することにより、受信したデータがどの装置によって、暗号化されたかが特定できる。

② 暗号文を復号せずに記録することによって、電文の

内容と、その発信元を示す証拠として用いることができる。

なぜならば暗号アルゴリズムまたは暗号鍵の少くとも一方が未公開であって、しかも、暗号化装置がハードウェア的に安全であれば、特定の装置を示す識別情報を含む暗号文を作成できるのは、その特定の装置だけであるからである。

たとえ、受信者側で、記録の偽造を試みても、受信者側装置で作れるのは、別な識別ワード（識別ワードは各装置、ICカード毎に固有であり、識別ワードが暗号化回路２への入力時に強制的に電文を合成されることに留意）を含んだ暗号文だけであり、偽造は困難である。次に取引の手続を第８図に従って説明する。

取引を行うには、顧客端末からセンタに送られる取引電文をICカード内で暗号化し、その暗号化電文Ｃを通信回線に送出する。これにより、第３者による取引電文の偽造が困難となる。

第６図に、鍵生成法の一例を示す。取引電文を暗号化する鍵65は、個人キーワードI62;秘密キーワードS61、乱数データR63により生成される。

個人キーワードとしては、使用者毎に設定された番号符号であり、例えば、口座番号が利用される。秘密キーワードとは、この通信ネットワークに共通な番号である。乱数データは、センタ側で発生され、取引番号を示すデータである。ここでの個人キーワードＩと乱数データとは、暗号通信に先立って、センタ、ユーザのICカード間で交換される。

MPU41はこれらキーワードI, S, Rに従って、例えば（Ｉ＋Ｓ＋Ｒ）なる排他的論理和64の演算を実行して暗号化の為のキーワードＫを生成する。そしてMPU41はこの暗号化キーワードＫを用い、例えばDESのような暗号化アルゴリズムに従って暗号化する。ここで秘密のキーワードＳをセンタも知らない乱数にすれば、キーワードＫは、第３者はもちろんユーザやセンサさえも知らない完全な秘密キーワードとすることが可能となる。

端末からICカードに入力された取引電文Ｍにはまず ICカード固有の識別番号Ｎが合成器70で合成される。その一例を第７図に示す。取引電文M71（ｍビット）と識別番号N72（ｎビット）とを直列合成してシリアルデータ74を合成する場合には、合成器70においてＭをｎビットシフトした後Ｎと加算処理すればよい（73はビットシフト手段である）。

例えば、N71がｎビット、M72がｍビットとしＮを付加された後の電文をＭ′とする時Ｍ′を次のように決めれば良い。

$M' = 2^n \cdot M + N$

Ｍ′はＭを上位ビット、Ｎを下位ビットとするｍ＋ｎビットのデータである。上記の例は最も単純な方法である。受信側でＭとＮを分離して取り出すことが出来るならば、他の任意の方法が適用可能である。

Ｎが付加された電文Ｍ′は、キーワードＫと暗号アルゴリズムに従って暗号化される。

暗号文はＮとＭに依存するので、これをＥ（N, M）と書く事にする。Ｅ（N, M）はリーダ・ライタを介して

端末に送られ、さらに端末からセンタへ送信される。暗号電文Ｅ（N, M）を受け取ったセンタ側端末は、これを端末に装填されたICカードに送り、カード内の復号器によって復号し、その結果であるＭ′をICカードから受け取る。さらにＭ′から電文Ｍと、識別番号Ｎを分離して、まずＮをチェックし、相手装置の認識を行なう。このために、センタは各ICカードの識別番号Ｎを、ユーザ名や、口座番号などと伴にデータベースに保管しておく必要がある。識別番号Ｎの確認が終わると、次は取引電文Ｍを調べその内容を実行する。そして、取引の記録として、取引の日付や取引番号など取引に関する情報と伴に、復号前の電文Ｅ（N, M）と鍵生成に必要な情報I, Rとをプリンタに出力する。同時にフロッピーディスクのような電子的な記憶装置に記録を残す事も可能である。

このように、記録にＥ（N, M）：I, Rを添えることにより、記録の証拠性は格段に向上する。その説明に入る前に本実施例の前提を明らかにしておく必要がある。まず、ユーザ、センタの各ICカードがハードウェア的に完全であって、内部のデータは、正当な手段以外では取り出せないとする。そして、カード識別子Ｎは、カードごとすべて異なるものとする。また暗号アルゴリズムは周知でもよいが、各取引毎の鍵は完全に秘密で、第３者はもちろん、ユーザ、センターの管理者さえも知らないものとする。これは既に述べたように鍵生成の秘密のパラメータＳをセンターの管理者も知らない乱数とすればよい。センサも知らない乱数をICカード内で作り出す手段としては例えば、センタが作った鍵ＳＣに、カード製造者が作ってカードに収めた秘密鍵ＳＭを加えたものとしてもよい。

Ｓ＝ＳＭ＋ＳＣ　（＋：排他的論理和）

このような前提の下ではＥ（N, M）を作れるのは識別子Ｎをもつ特定のカードだけとなる。なぜならば、まず他のユーザカードではＮおよび鍵Ｋを持たないのでＥ（N, M）の偽造はできない。またセンタが偽造を試みる場合を考えてみても、ICカードを用いる限りほかのユーザの場同様Ｅ（N, M）の複製は困難である。

一方、センタがデータベースから得たＮを用いてカードで外で暗号化を試みても、限Ｋの値を知らないので、Ｅ（N, M）の偽造はできない。以上のことから

Ｅ（N, M）は付加する事により取引記録の証拠能力は非常に高まる。そして、後日取引に関するトラブルが生じた時にはこの記録によってトラブルの解決を図ることができる。

ここまでの説明では、ユーザからセンタへの電文に関する内容証明について扱って来た。これと全く同様にして、センタからの暗号電文をユーザ側端末で記録するこ

9

とにより、センタからの電文の送信事実の証明とすることも可能である。なぜならばセンタ側ICカードの内部で電文が暗号化される時、センタ側ICカード固有の識別番号N′が電文に付加されるからである。

次に本発明の第２の実施例として、暗号化及び復号化のアルゴリズムをセンターの管理者及びユーザに対しても秘密にする場合を説明する。第２の実施例もシステム構成及び取引電文のやりとりの手順、鍵Kの配送手順は第１の実施例の場合と同じである。ただし第２の実施例においては、鍵Kの値を通信の当業者であるユーザ及びセンターの管理者は知っていてもかまわない。ただし暗復号のアルゴリズムはユーザもセンターの管理者も知らないものとする。例えばカード製造者がアルゴリズムを秘密にして実装する場合がこの場合に相当する。

このような条件の下でユーダがセンタに対して、暗号電文Ｅ（N, M）を送った時にもやはり、Ｅ（N, M）はNを識別番号とするICカード内でしか生成できない。したがってセンタはＥ（N, M）を記録することによって、ユーザから電文Mが送信された事実を示す証拠として使うことができる。

また逆に、センタからユーザへの電文の通信事実を示す証拠として、ユーザはセンタからの暗号電文を記録することができることは第１の実施例の場合と同様である。

第１と第２の実施例からわかるように、本発明による暗号器で生成された暗号文が電文送信事実を示す証拠として有効に作用するためには、番号化鍵と暗・復号化のアルゴリズムの少なくとも一方をユーザおよびセンタが知らない完全な秘密としなければならない。さもなければ、鍵と識別子Nとアルゴリズムを ICカード外部で用いて、偽の電文Ｅ（N, M）を作成することが、少なくともセンタにとっては比較的容易となる。センタに充分信頼がおけない場合には、Ｅ（N, M）の証拠としての能力が低められてしまう。

以上を述べてきた実施例においては、復号化された電文を電文Mとカード識別番号Nに再分離する機能を、カード外で実現するものであったが、この再分離機能をカード内で実現し、カード外へは分離されたNとMが出力される構成であっても本発明の目的である取引証明の現実は達成される。また、本発明の特徴を最も良く実現する暗号装置の形態の一つはカード形で携帯可能なもの、具体的にはICカードであったが、本発明の実施例と同様

10

な機能を組み込み可能な任意の暗号装置であるなら何ら制限はない。

又、合成手段では、実施例のように、２つの電文を単純に直列合成するという処理だけでなく、発信元、送信元で同一の処理を施すことがわかっていれば、どのような処理であっても原則として構わない。言い換えると、再分離可能な処理ということもできる。

なお、ここでの送信元とは、受信電文を証拠として用いるレベルを指し、必ずしも全ての受信端末、オーペレータが知っている必要はない。

又、上記の実施例では、平文に対して、装置（ICカード）固有の識別ワードを合成したが、電文に対して取引を特定するワードを付与することが技術的に価値がある。例えば、平文に対して、“鍵”を用いて暗号化を施し、この結果を平文と合成するものである。このようにして得られた電文を暗号化装置により暗号化して外部へ送出することが好ましい。

但し、暗号装置（ICカード）の処理能力からして、ICカード外部に設けられている暗号化手段により合成手段を暗号化することも好ましい。ここでの暗号化手段は、通常、外線に電文（信号）を送出する際に、設けられているものを指す。

又、上記平文の暗号化は、上述の実施例と同様に、ICカード内のMPUにより実現される。

［発明の効果］

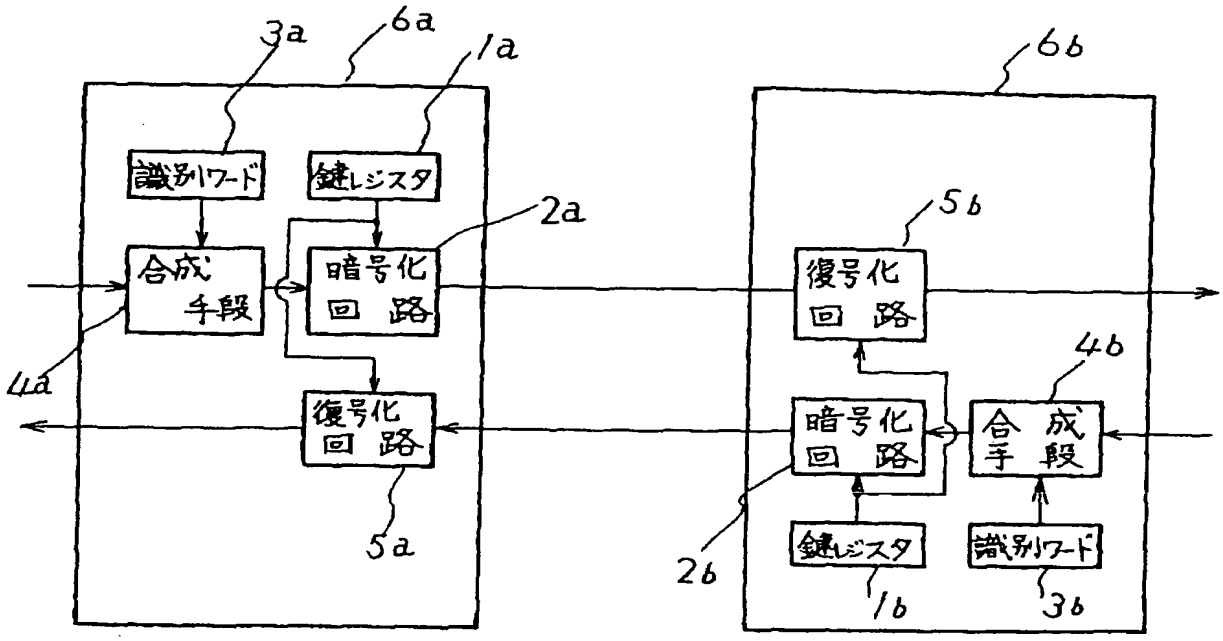
本発明によれば、暗号電文を復号すれば、その電文を作成した、暗号装置が確定するので、これを取引証明に利用することによってユーザ・センタ間の取引に関するトラブルを解決することが可能となる。

【図面の簡単な説明】

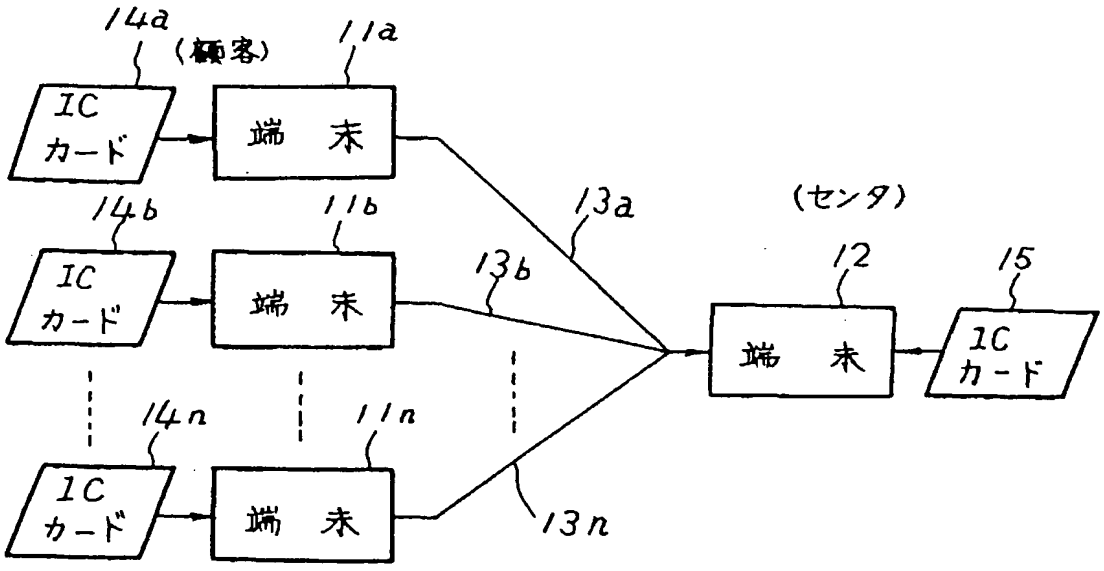
第１図は、本発明の一実施例に係る暗号装置を対向して用いた場合のブロック図、第２図は、本発明をICカードに適用した場合のシステム構成を示す図、第３図は、第２図に示すシステムでのユーザ端末の構成を示す図、第４図は同システムでのセンタ端末の構成を示す図、第５図は、ICカードの構成を示す図、第６図は、鍵の生成法を説明するための図、第７図は、合成手段の構成を示す図、第８図は、第２図のシステムの手続の概念を示す図である。

１……鍵レジスタ、２……暗号化回路、３……識別ワードレジスタ、４……合成手段、５……復号化回路、６……暗号装置

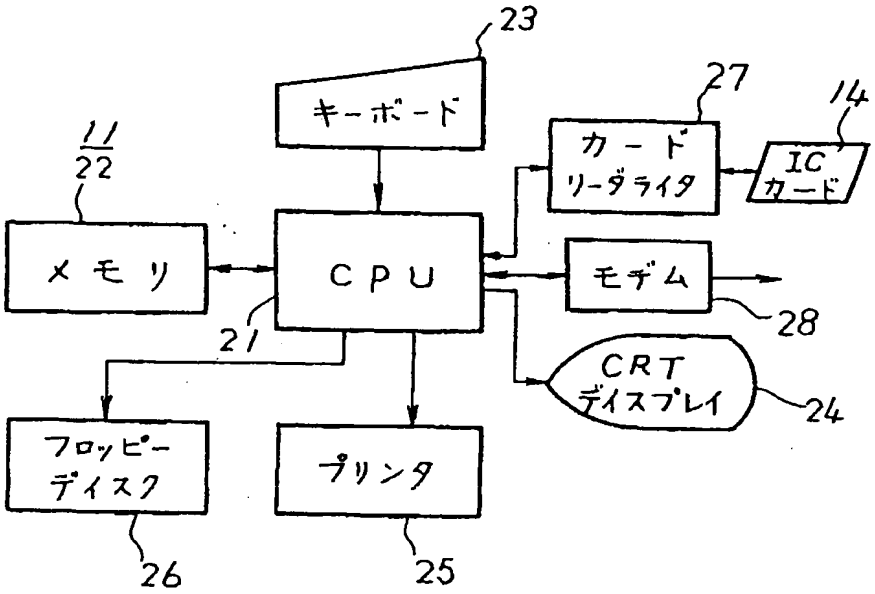
【第１図】


3a
6a
1a
識別ワード
鍵レジスタ
2a
合成手段
暗号化回路
4a
復号化回路
5a
6b
5b
復号化回路
4b
暗号化回路
合成手段
2b
鍵レジスタ
識別ワード
1b
3b

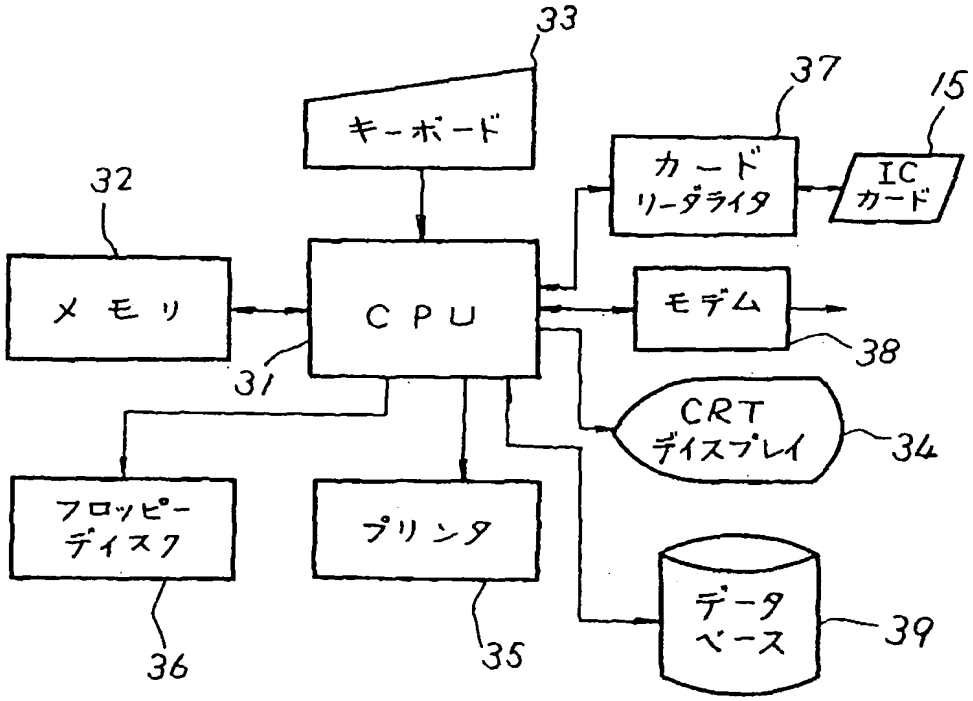
【第２図】


14a
(顧客)
11a
ICカード
端末
14b
11b
ICカード
端末
14n
11n
ICカード
端末
13a
13b
13n
(センタ)
12
15
端末
ICカード

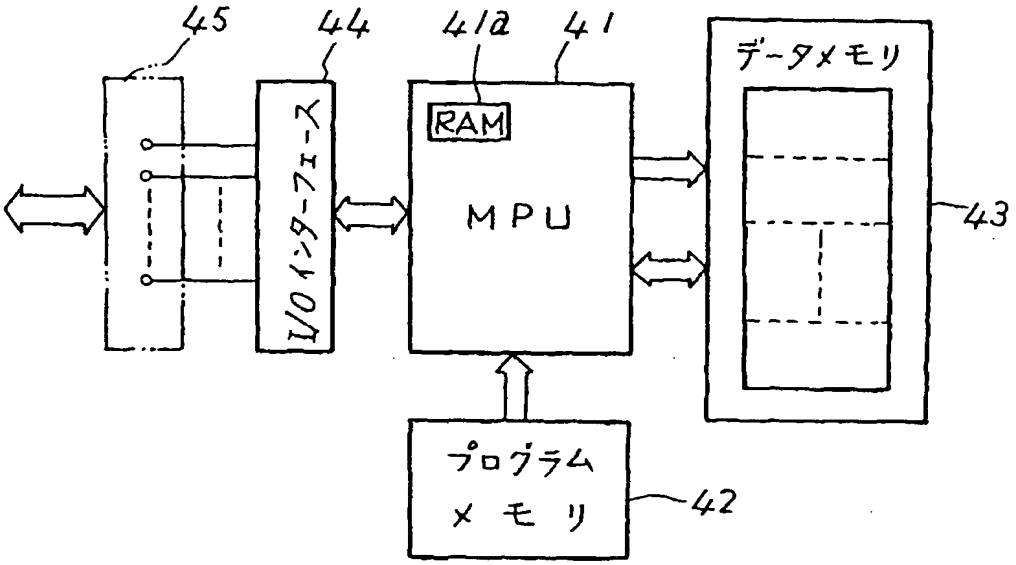
【第３図】


23
キーボード
27
14
カード
リーダライタ
IC
カード
11
22
メモリ
CPU
モデム
28
21
CRT
ディスプレイ
24
フロッピー
ディスク
プリンタ
26
25

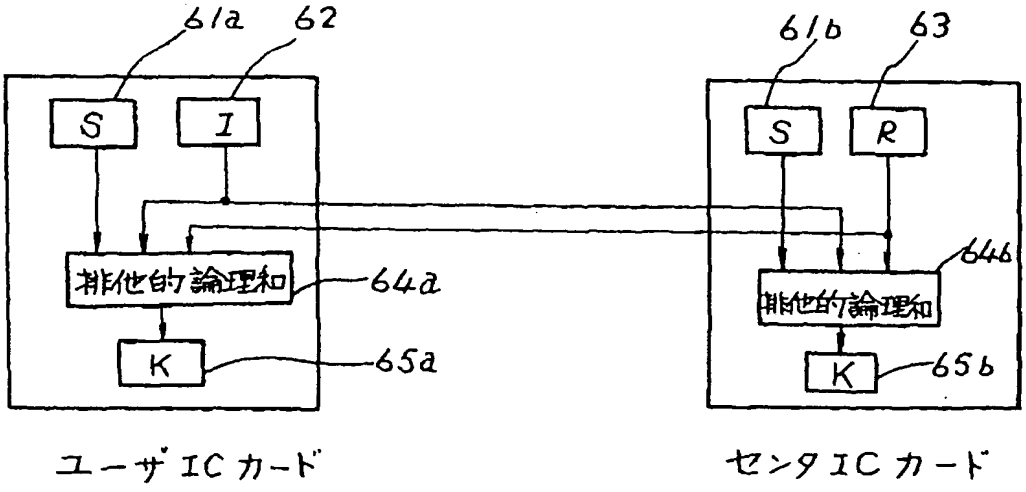
【第４図】


33
キーボード
37
15
カード
リーダライタ
IC
カード
32
メモリ
CPU
モデム
38
31
CRT
ディスプレイ
34
フロッピー
ディスク
プリンタ
データ
ベース
39
36
35

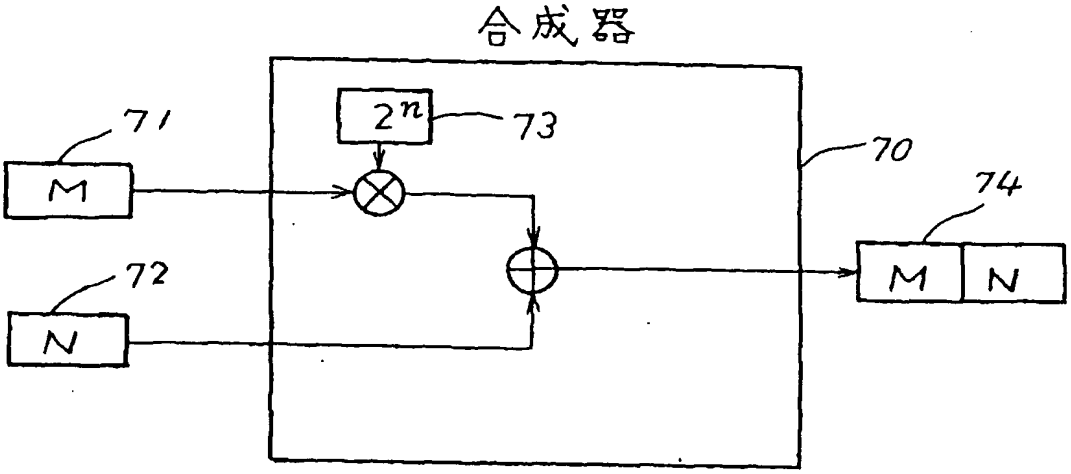
【第５図】


45
44
41a
41
データメモリ
RAM
I/Oインターフェース
MPU
43
プログラム
メモリ
42

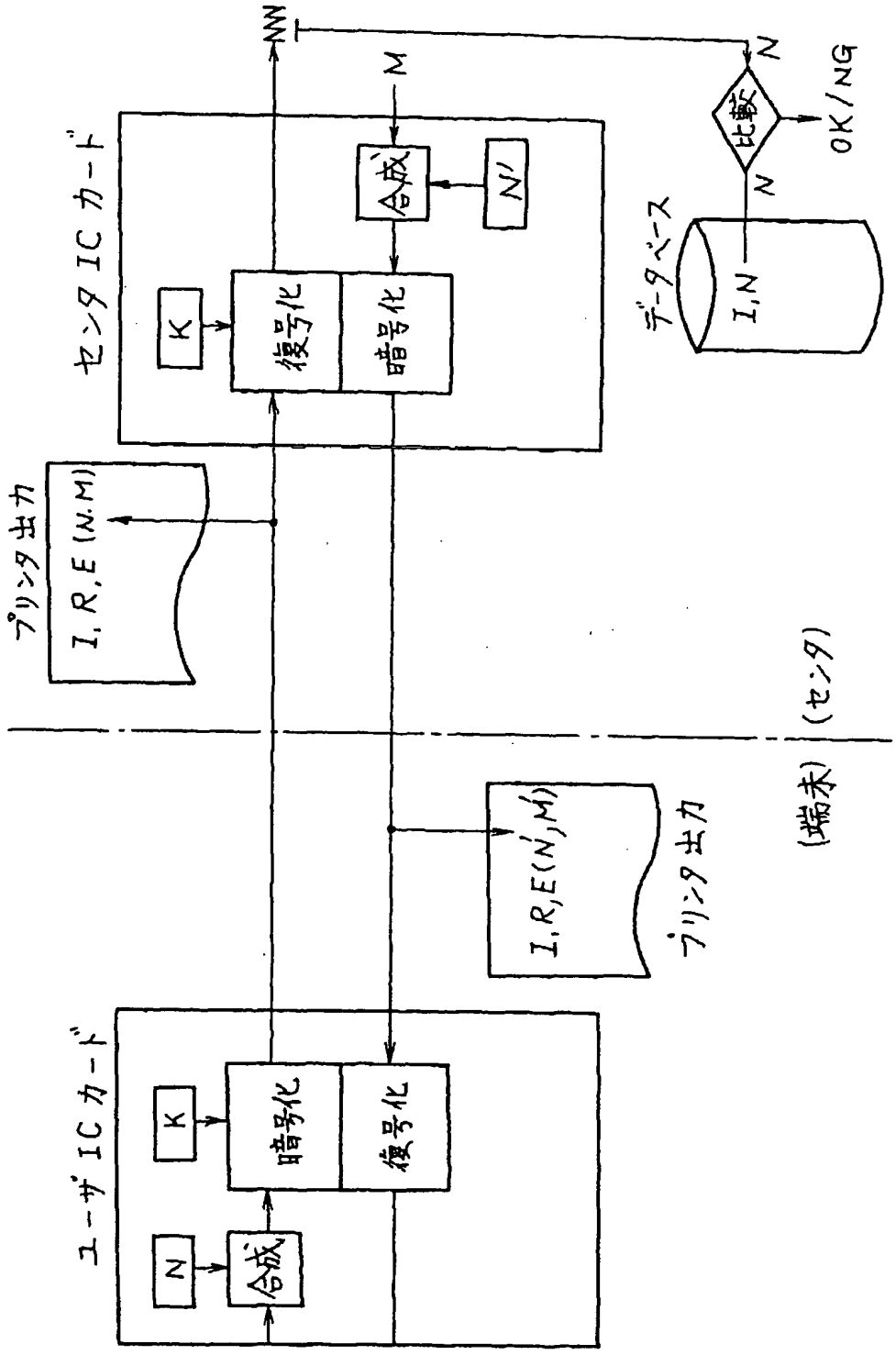
【第６図】


61a
62
61b
63
S
I
S
R
排他的論理和
64a
64b
K
65a
K
65b
ユーザICカード
センタICカード

【第７図】



【第８図】


NN
M
N
センタ IC カード
合成
N'
K
復号化
暗号化
比較
OK/NG
データベース
I,N
プリンタ出力
I,R,E(N,M)
(センタ)
(端末)
I,R,E(N',M)
プリンタ出力
ユーザ IC カード
K
暗号化
復号化
N
合成

フロントページの続き

(72)発明者　水谷　博之
川崎市幸区小向東芝町１　株式会社東芝
総合研究所内

(56)参考文献　特開　昭60－208137（ＪＰ，Ａ）
特開　昭56－143744（ＪＰ，Ａ）
特開　昭59－769（ＪＰ，Ａ）